Forescout Banking on Security – leveraging device data to manage risk in Financial Services

Learn more from a webinar featuring Chase Cunningham of Forrester: Zero Trust Security in the Age of IoT & OT.

Don’t just see it. Secure it.

© 2021 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products or service names may be trademarks or service marks of their respective owners. Version 01_21.

Step 1
Identify the attack surface
Lack of full-visibility into connected users, devices, applications and workloads prevents you from being able to design and manage efficient and secure network flows. To realize the full extent of your attack surface, you must discover, classify and assess the risk of every connected thing.

Step 2
Map data flows and system interdependencies
You must be able to see the network traffic flows of devices and the protocols being used to communicate. Traffic-flow data married to how entities communicate across all networks helps you establish communication baselines, detect anomalous behavior and implement Zero Trust policies.

Step 3
Correlate user, device and posture data to determine least privilege access
Least privilege access is a core principle of Zero Trust. You must have the ability to continuously identify and verify the user, device and its security state for defining effective and dynamic least privilege network access.

Step 4
Build and test Zero Trust policies
Design Zero Trust control policies and simulate them before enforcement to minimize potential productivity and security impact. Today’s leading solutions provide policy-based segmentation enforcement that automatically isolates enterprise things to minimize breach impact.

Step 5
Orchestrate, monitor and automate response
Insufficient security tool integration and information exchange create blind spots in your ZTX strategy. An efficient solution will automate context sharing across all enterprise security tools and execute controls across multivendor physical and virtual environments.

FAST FACT
Nearly 45% of IoT devices on networks are printers... and they are often on the same segment as POS systems.1

1 Personal Banking on Security — Leveraging device data to manage risk in Financial Services

ZERO TRUST
QUICK START
A 5-Step Guide to Rapid Implementation

Step 1
Identify the attack surface
Lack of full-visibility into connected users, devices, applications and workloads prevents you from being able to design and manage efficient and secure network flows. To realize the full extent of your attack surface, you must discover, classify and assess the risk of every connected thing.

Step 2
Map data flows and system interdependencies
You must be able to see the network traffic flows of devices and the protocols being used to communicate. Traffic-flow data married to how entities communicate across all networks helps you establish communication baselines, detect anomalous behavior and implement Zero Trust policies.

Step 3
Correlate user, device and posture data to determine least privilege access
Least privilege access is a core principle of Zero Trust. You must have the ability to continuously identify and verify the user, device and its security state for defining effective and dynamic least privilege network access.

Step 4
Build and test Zero Trust policies
Design Zero Trust control policies and simulate them before enforcement to minimize potential productivity and security impact. Today’s leading solutions provide policy-based segmentation enforcement that automatically isolates enterprise things to minimize breach impact.

Step 5
Orchestrate, monitor and automate response
Insufficient security tool integration and information exchange create blind spots in your ZTX strategy. An efficient solution will automate context sharing across all enterprise security tools and execute controls across multivendor physical and virtual environments.

Zero Trust Principles
Complete visibility is foundational
Incorporate identity beyond users and IAM
Segmentation is key – enforce policy everywhere

"A key piece of this whole thing is knowing what is supposed to be occurring, being able to control it and then responding to it." — Dr. Chase Cunningham, Principal Analyst at Forrester

Learn more from a webinar featuring Chase Cunningham of Forrester: Zero Trust Security in the Age of IoT & OT.

WATCH WEBINAR